REMARKS

This Application has been carefully reviewed in light of the Final Office Action mailed January 12, 2005. Claims 1-10 are pending in the Application. In the Final Office Action, the Examiner rejected Claims 1-10. Applicant has amended Claim 6. Applicant submits that no new matter has been added with these amendments. As described below, Applicant believes all claims to be allowable over the cited references. Therefore, Applicant respectfully requests reconsideration and full allowance of all pending claims.

Section 102 Rejections

The Examiner rejects Claims 1-2, 4-6, and 8-10 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,163,097 issued Pegg ("*Pegg*"). For the following reasons, Applicant respectfully requests reconsideration and allowance of Claims 1-2, 4-6, and 8-10.

With respect to Claims 1-2, 4-6, and 8-10, Applicant has considered the Examiner's Response to Arguments in the Final Office Action but continues to believe that *Pegg* does not disclose, teach, or suggest each and every element recited in Applicant's claims. For example, independent Claim 1, of the present Application, recites, *inter alia*, the following combination of elements:

- selecting a table key value to be used as an index into an encryption selection table . . . specifying at least one of a plurality of encryption methods to be used to encrypt a data message;
- encrypting the data message using the encryption method associated with the table key value; and
- transmitting the encrypted data message over a data communication network.

Thus, at a minimum, Claim 1 clearly recites a method for communicating a data message that includes an "encryption selection table specifying at least one of a plurality of encryption methods to be used to encrypt a data message." Claim 1 further recites both "encrypting the data message" using a selected encryption method and "transmitting the encrypted data message over a data communication network." In the Final Office Action, the Examiner

continues to rely on *Pegg* for disclosure of the combination of recited elements. Applicant respectfully submits, however, that *Pegg* merely discloses a limited access system that includes an additional level of security for verifying the identity of a user of an ATM machine. To the extent that *Pegg* discloses the use of a cipher algorithm by an authorization center to "substantially [disguise] the user's access key from onlookers," the use of the cipher algorithm is limited to the machine-generation of a dynamic access code that may be matched against a human generated dynamic access code in determining whether to grant a user access to their account through the ATM machine. (Column 4, lines 48-52; Column 2, lines 53-63). *Pegg* does not disclose, teach, or suggest, however, the above recited combination of features.

Specifically and as discussed in Applicant's previous Response to Office Action submitted on July 30, 2004, *Pegg* discloses "an authorization center coupled to an access code entry means (e.g., telephone dial, ISDN hone keypad, ATM keypad, a dual tone multiple frequency keypad, touch or scribe sensitive screen, speech recognition device, etc.)." (Column 3, lines 3-7). A unique access key, such as a pin, is assigned to the user. (Column 4, lines 9-10). "The user preselects one of the cipher algorithms 118 from the pool of selectable cipher algorithms 110 when the access key is first assigned to the user." (Column 4, lines 20-23). Thus, the user predetermines which cipher algorithm 118 will be used when the user seeks access to account information through the ATM. In operation, the ATM prompts the user to enter a non-machine generated access code 123 when the user seeks access to the user's account information. (Column 5, lines 24-26). The non-machine generated access code 123 "is generated from memory by the user without the necessity of a separate computer." (Column 4, lines 38-41). Thus, the user manually generates the access code 123 using the selected cipher algorithm and at least the user's access key and one or more dynamic variables and enters the non-machine generated access code via a keypad or other input device. (Column 4, lines 30-33; Column 5, lines 29-32).

For the purpose of verifying the identity of the user using the access code entry means (i.e., ATM), the authorization center maintains user account information 104 in the form of a table that includes "account ID's; user access keys 106; user algorithm index numbers 108;

user selectable cipher algorithms 110; and dynamic variables 112." (Column 4, lines 1-4). The authorization center then proceeds to generate a corresponding access code based on the stored data. (Column 5, lines 48-51). "After the user 101 and the authorization center generate access codes, 123, 124, they are compared to determine whether a match exists." (Column 5, lines 5-8). "A match indicates a valid access code." (Column 5, line 8). Accordingly, Applicant respectfully submits that *Pegg* merely discloses a limited access system that includes an additional level of security for verifying the identity of a user of an ATM machine. The additional level of security requires that both the user and the access system independently generate access codes 123 and 124 that are "compared to determine if a match exists." (Column 5, lines 5-8). The *Pegg* system is in contrast to prior systems that merely use a bank-issued PIN and an account number for accessing ATM's. (Column 1, lines 17-20).

With respect to the Examiner's rejection of Claim 1, the Examiner seems to rely upon the generation of the non-machine generated access code 123 for disclosure of some of the recited claim elements and the generation of the machine generated access code 124 for disclosure of other of Applicant's recited claim elements. Specifically, the Examiner states:

> The Examiner has interpreted the encryption or encipherment of the data message to be the algorithm that is used to masque the original access key with regards to future attempts by the user to access the system. As previously cited by Examiner, *Pegg* (Column 4, lines 48-52), the purpose of the algorithm is to substantially disguise the user's access key. In this sense, this data message containing the user's access key is encrypted using the user's previously selected algorithm.
>
> This message is also transmitted over a data communication network to the user.

(Final Office Action, page 3). Thus, with respect to Applicant's step reciting "selecting a table key value to be used as an index into an encryption selection table . . . " and Applicant's step reciting "encrypting the data message using the encryption method associated with the table key value," the Examiner appears to rely upon *Pegg's* disclosure with respect to non-machine generated access code 123. With respect to Applicant's step reciting "transmitting

the encrypted data message over a data communication network," however, the Examiner appears to rely upon *Pegg's* disclosure with respect to machine generated access code 124. Applicant respectfully submits that such an approach is improper since it fails to give full credence to the combination of elements recited in Applicant's Claim 1. Applicant reiterates that the standard for maintaining a rejection under § 102 requires that "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131 (*emphasis added*). Furthermore, "[a]ll words in a claim must be considered in judging the patentability of that claim against prior art." M.P.E.P. § 2143.03 (citing *In re Wilson*, 424 F.2d 1382, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970)).

Neither of *Pegg's* disclosure with respect to the non-machine generated access code 123 nor *Pegg's* disclosure with respect to the machine generated access code 124 satisfy the particular combination of elements recited in Applicant's Claim 1. With respect to the non-machine generated access code 123 of *Pegg*, the user manually generates the non-machine-generated access code 123 using the selected cipher algorithm and at least the user's access key and one or more dynamic variables. (Column 4, lines 30-33; Column 5, lines 29-32). Because the pre-selected cipher algorithm is pulled from the user's memory, the user of the *Pegg* system does not "select a table key value to be used as an index into an encryption selection table . . . specifying at least one of a plurality of encryption methods to be used to encrypt a data message," as recited in Applicant's Claim 1. For similar reasons, the non-machine generated access code 123 also cannot be said to the encrypted "using the encryption method associated with the table key value," as recited in Applicant's Claim 1. For at least these reasons, Applicant respectfully submits that the non-machine generated access code 123 is not the equivalent of Applicant's encrypted data message.

The machine generated access code 124 of *Pegg* is also not the equivalent of Applicant's encrypted data message. As discussed above, the machine generated access code 124 is generated based on stored data and corresponds generally with the non-machine access

code 123. (Column 5, lines 48-51). Accordingly, even though a "pool of cipher algorithms 110 [that] includes a list of simple yet effective coding schemes" is used to generate the machine generated access code 124" (Column 4, lines 48-52), the authorization center of *Pegg* merely compares the machine generated access code 124 to the non-machine generated access code 123 "to determine whether a match exists." (Column 5, lines 5-8). *Pegg* does not disclose any further use of the machine generated access code 124. Accordingly, Applicant submits that *Pegg* does not disclose, teach, or suggest "transmitting the encrypted data message over a data communication network," as recited in Applicant's Claim 1.

For at least these reasons, Applicant respectfully requests reconsideration and allowance of independent Claim 1.

The Examiner also relies on *Pegg* for disclosure of Applicant's independent Claim 6. Applicant respectfully submits, however, that *Pegg* does not disclose teach, or suggest each and every limitation recited in Applicant's amended Claim 6. For example, Claim 6 recites "an encryption selection table accessible using a key value, the encryption selection table specifying at least one of the plurality of encryption programs to be used for each key value." Claim 6 also recites "a communication interface operable to transmit the encrypted message to the user of the device, the encrypted message encrypted using the at least one encryption program specified in the encryption selection table." As discussed above with regard to Claim 1, however, neither of *Pegg's* non-machine generated access code 123 nor *Pegg's* machine generated access code 124 are the equivalent of Applicant's encrypted message. Accordingly, for similar reasons to those discussed above with regard to Claim 1, Applicant respectfully submits that *Pegg* does not disclose, teach, or suggest the combination of features and elements recited in Applicant's independent Claim 6.

Claims 2 and 4-5 depend from independent Claim 1, which Applicant has shown above to be allowable. Claims 8-10 depend from independent Claim 6, which Applicant has shown above to be allowable. Since Claims 2, 4-5, and 8-10 incorporate the limitations of their respective independent claims, Claims 2, 4-5, and 8-10 are allowable for at least this

reason. Additionally, Applicant respectfully submits that Claims 2, 4-5, and 8-10 also recite features that are not disclosed, taught, or suggested in *Pegg*. Because Applicant has shown the independent claim to be allowable, however, Applicant has not provided detailed arguments with respect to Claims 2, 4-5, and 8-10. Applicant remains ready to do so if it becomes appropriate.

Section 103 Rejections

The Examiner rejects Claims 3 and 7 under 35 U.S.C. § 103(a) as being unpatentable over *Pegg*. For the following reasons, Applicant respectfully requests reconsideration and allowance of Claims 3 and 7.

First, Claims 3 and 7 depend from independent Claims 1 and 6, respectively, which Applicant respectfully submits have been shown above to be allowable. Since Claims 3 and 7 incorporate the limitations of their respective independent claims, Claims 3 and 7 are allowable for at least this reason.

Second, Applicant respectfully submits that Claims 3 and 7 also recite features that are not disclosed, taught, or suggested in the cited art. With respect to Claim 3, the Examiner acknowledges that *Pegg* does not disclose, teach, or suggest "encrypting the data message a second time using the second encryption method prior to transmitting the encrypted message." Rather, the Examiner takes Official Notice that the recited features are well known in the art at the time of the invention and provides citations to U.S. Patent No. 5,742,686 issued to Finley ("*Finley*"), U.S. Patent No. 5,343,527 issued to Moore ("*Moore*"), and U.S. Patent No. 6,091,818 issued to Campinos ("*Campinos*") as examples of the art at the time of invention. Applicant continues to respectfully traverse the rejection of the claims on this basis.

The mere fact that references can be combined does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills,* 916 F.2d 680 (Fed. Cir. 1990). The showing must be clear and particular. *See, e.g.,*

C.R. Bard v. M3 Sys., Inc., 48 U.S.P.Q.2d 1225, 1232 (Fed. Cir. 1998). The Examiner has not provided adequate evidence that one of ordinary skill in the art at the time of the present invention would have been motivated to modify the limited access system disclosed in *Pegg* to include the teachings disclosed in *Finley*, *Moore*, or *Campinos*. The Examiner merely speculates "it would have been obvious" to modify the limited access system disclosed in *Pegg* to "second encrypt the data using a selected algorithm from an algorithm table before transmitting it to another party because it would provide an extra layer of security in the encryption." (Office Action, page 7). As discussed above, however, *Pegg* discloses that a user of the limited access system manually generates the access code 123 using the selected cipher algorithm. (Column 4, lines 30-33; Column 5, lines 29-32). Thus, were a second encryption method used by the limited access system disclosed in *Pegg*, the user would be required to remember both a first and a second cipher algorithm and the order in which they should be applied to generate the access code. *Pegg* discloses, however, that "[t]he pool of cipher algorithms 110 includes a list of simple yet effective coding schemes." (Column 4, lines 48-52). Accordingly, Applicant respectfully submits that one of ordinary skill in the art at the time of Applicant's invention would not have been motivated to modify the limited access system disclosed in *Pegg* as suggested by the Examiner.

For at least these reasons Applicant respectfully requests reconsideration and allowance of Claims 3 and 7.

CONCLUSION

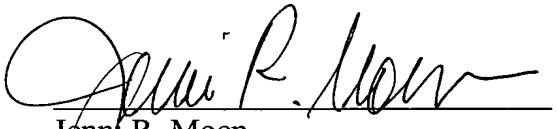
Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicant respectfully requests full allowance of all pending claims.

If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the Examiner is invited to contact Jenni R. Moen, Attorney for Applicant, at the Examiner's convenience at (214) 953-6809.

Although no fees are believed to be due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Jenni R. Moen
Reg. No. 52,038
(214) 953-6809

Date: March 8, 2005

Correspondence Address:

at Customer No. **05073**